Studies, cyber crimes in 2013 cost more than $100 billion in the United States and, roughly, half a trillion dollars globally.

Mr. Speaker, Congress needs to resolve these problems by working together to improve our Nation's cyber defenses rather than having President Obama try to solve the problem one executive order at a time, and that is exactly what the House is doing this week. Determined to protect the American people from future cyber attacks, last night, the House passed one bipartisan bill—and it will vote on another today—which seeks to balance security while protecting privacy.

Mr. Speaker, after years of inaction, the White House has indicated it is willing to work with Congress on this issue, signaling that we may finally put the policies in place that are necessary to protect our digital world in the 21st century.

□ 0915

NATIONAL CYBERSECURITY PROTECTION ADVANCEMENT ACT OF 2015

GENERAL LEAVE

Mr. MCCAUL. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks and include extraneous materials on the bill, H.R. 1731.

The SPEAKER pro tempore (Mr. RATCLIFFE). Is there objection to the request of the gentleman from Texas?

There was no objection.

The SPEAKER pro tempore. Pursuant to House Resolution 212 and rule XVIII, the Chair declares the House in the Committee of the Whole House on the state of the Union for the consideration of the bill, H.R. 1731.

The Chair appoints the gentleman from Georgia (Mr. WOODALL) to preside over the Committee of the Whole.

□ 0916

IN THE COMMITTEE OF THE WHOLE

Accordingly, the House resolved itself into the Committee of the Whole House on the state of the Union for the consideration of the bill (H.R. 1731) to amend the Homeland Security Act of 2002 to enhance multi-directional sharing of information related to cybersecurity risks and strengthen privacy and civil liberties protections, and for other purposes, with Mr. WOODALL in the chair.

The Clerk read the title of the bill.

The CHAIR. Pursuant to the rule, the bill is considered read the first time.

The gentleman from Texas (Mr. MCCAUL) and the gentleman from Mississippi (Mr. THOMPSON) each will control 30 minutes.

The Chair recognizes the gentleman from Texas.

Mr. MCCAUL. Mr. Chairman, I yield myself such time as I may consume.

I am pleased to bring to the floor H.R. 1731, the National Cybersecurity Protection Advancement Act, a proprivacy, prosecurity bill that we desperately need to safeguard our digital networks.

I would like to commend the subcommittee chairman, Mr. RATCLIFFE, for his work on this bill as well as our minority counterparts, including Ranking Member THOMPSON and subcommittee Ranking Member RICHMOND for their joint work on this bill. This has been a noteworthy, bipartisan effort. I would also like to thank House Permanent Select Committee on Intelligence Chairman DEVIN NUNES and Ranking Member ADAM SCHIFF for their input and collaboration. Lastly, I would like to thank Committee on the Judiciary Chairman GOODLATTE and Ranking Member CONYERS for their contribution.

Make no mistake, we are in the middle of a silent crisis. At this very moment, our Nation's businesses are being robbed, and sensitive government information is being stolen. We are under siege by a faceless enemy whose tracks are covered in cyberspace.

Sophisticated breaches at companies like Anthem, Target, Neiman Marcus, Home Depot, and JPMorgan have compromised the personal information of millions of private citizens. Nation-states like Iran and North Korea have launched digital bombs to get revenge at U.S.-based companies, while others like China are stealing intellectual property. We recently witnessed brazen cyber assaults against the White House and the State Department, which put sensitive government information at risk.

In the meantime, our adversaries have been developing the tools to shut down everything from power grids to water systems so they can cripple our economy and weaken our ability to defend the United States.

This bill will allow us to turn the tide against our enemies and ramp up our defenses by allowing for greater cyber threat information sharing. This bill will strengthen the Department of Homeland Security's National Cybersecurity and Communications Integration Center, or NCCIC. The NCCIC is a primary civilian interface for exchanging cyber threat information, and for good reason. It is not a cyber regulator. It is not looking to prosecute anyone, and it is not military or a spy agency. Its sole purpose, Mr. Chairman, is to prevent and respond to cyber attacks against our public and private networks while aggressively protecting Americans' privacy.

Right now we are in a pre-9/11 moment in cyberspace. In the same way legal barriers and turf wars kept us from connecting the dots before 9/11, the lack of cyber threat information sharing makes us vulnerable to an attack. Companies are afraid to share because they do not feel they have the adequate legal protection to do so.

H.R. 1731 removes those legal barriers and creates a safe harbor, which will encourage companies to voluntarily exchange information about attacks against their networks. This will allow both the government and private sector to spot digital attacks earlier and keep malicious actors outside of our networks and away from information that Americans expect to be defended.

This bill also puts privacy and civil liberties first. It requires that personal information of our citizens be protected before it changes hands—whether it is provided to the government or exchanged between companies—so private citizens do not have their sensitive data exposed.

Significantly, both industry and privacy groups have announced their support for this legislation because they recognize that we need to work together urgently to combat the cyber threat to this country.

Today, we have a dangerously incomplete picture of the online war being waged against us, and it is costing Americans their time, money, and jobs. It is time for us to safeguard our digital frontier. This legislation is a necessary and vital step to do exactly that.

Mr. Chairman, before I reserve the balance of my time, I would like to enter into the RECORD an exchange of letters between the chairman of the Committee on the Judiciary, Mr. GOODLATTE, and myself, recognizing the jurisdictional interest of the Committee on the Judiciary in H.R. 1731.

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON THE JUDICIARY,
Washington, DC, April 21, 2015.

Hon. MICHAEL MCCAUL,
Chairman, Committee on Homeland Security, Washington, DC.

DEAR CHAIRMAN MCCAUL: I am writing with respect to H.R. 1731, the ''National Cybersecurity Protection Advancement Act of 2015.'' As a result of your having consulted with us on provisions in H.R. 1731 that fall within the Rule X jurisdiction of the Committee on the Judiciary, I agree to waive consideration of this bill so that it may proceed expeditiously to the House floor for consideration.

The Judiciary Committee takes this action with our mutual understanding that by foregoing consideration of H.R. 1731 at this time, we do not waive any jurisdiction over the subject matter contained in this or similar legislation, and that our Committee will be appropriately consulted and involved as the bill or similar legislation moves forward so that we may address any remaining issues in our jurisdiction. Our Committee also reserves the right to seek appointment of an appropriate number of conferees to any House-Senate conference involving this or similar legislation, and asks that you support any such request.

I would appreciate a response to this letter confirming this understanding, and would ask that a copy of our exchange of letters on this matter be included in the Congressional Record during Floor consideration of H.R. 1731.

Sincerely,

BOB GOODLATTE,
Chairman.

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC, April 21, 2015.

Hon. BOB GOODLATTE,
Chairman, Committee on Judiciary,
Washington, DC.

DEAR CHAIRMAN GOODLATTE: Thank you for your letter regarding H.R. 1731, the ''National Cybersecurity Protection Advancement Act of 2015.'' I appreciate your support in bringing this legislation before the House of Representatives, and accordingly, understand that the Committee on Judiciary will not seek a sequential referral on the bill.

The Committee on Homeland Security concurs with the mutual understanding that by foregoing a sequential referral of this bill at this time, the Judiciary does not waive any jurisdiction over the subject matter contained in this bill or similar legislation in the future. In addition, should a conference on this bill be necessary, I would support your request to have the Committee on Judiciary represented on the conference committee.

I will insert copies of this exchange in the Congressional Record during consideration of this bill on the House floor. I thank you for your cooperation in this matter.

Sincerely,

MICHAEL T. MCCAUL,
Chairman, Committee on Homeland Security.

Mr. MCCAUL. With that, I urge my colleagues to support this important legislation.

I reserve the balance of my time.

Mr. THOMPSON of Mississippi. Mr. Chairman, I yield myself such time as I may consume.

I rise in support of H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015.

Mr. Chairman, every day U.S. networks face hundreds of millions of cyber hacking attempts and attacks. Many of these attacks target large corporations and negatively impact consumers. They are launched by common hackers as well as nation-states. As the Sony attack last year demonstrated, they have a great potential for harm and put our economy and homeland security at risk.

Last week, it was reported that attacks against SCADA industrial control systems rose 100 percent between 2013 and 2014. Given that SCADA systems are essential to running our power plants, factories, and refineries, this is a very troubling trend.

Just yesterday, we learned about an advanced persistent threat that has targeted high-profile individuals at the White House and State Department since last year. According to an industry expert, this cyber threat—nicknamed CozyDuke—includes malware, information-stealing programs, and antivirus back doors that bear the hallmarks of Russian cyber espionage tools.

Mr. Chairman, cyber terrorists and cyber criminals are constantly innovating. Their success is dependent on their victims not being vigilant and protecting their systems. Cyber terrorists and cyber criminals exploit bad practices, like opening attachments and clicking links from unknown senders. That is why I am pleased that H.R. 1731 includes a provision authored by Representative WATSON COLEMAN to authorize a national cyber public awareness campaign to promote greater cyber hygiene.

Another key element of cybersecurity is, of course, information sharing about cyber threats. We have seen that when companies come forward and share their knowledge about imminent cyber threats, timely actions can be taken to prevent damage to vital IT networks. Thus, cybersecurity is one of those places where the old adage ''knowledge is power'' applies.

That is why I am pleased H.R. 1731 authorizes private companies to voluntarily share timely cyber threat information and malware with DHS or other impacted companies. Under H.R. 1731, companies may voluntarily choose to share threat information to prevent future attacks to other systems.

I am also pleased that the bill authorizes companies to monitor their own IT networks to identify penetrations and take steps to protect their networks from cyber threats. H.R. 1731 builds on bipartisan legislation enacted last year that authorized the Department of Homeland Security's National Cybersecurity and Communications Integration Center, commonly referred to as NCCIC.

H.R. 1731 was unanimously approved by the committee last week and represents months of outreach to a diverse array of stakeholders from the private sector and the privacy community. Importantly, H.R. 1731 requires participating companies to make reasonable efforts prior to sharing to scrub the data to remove information that could identify a person when that person is not believed to be related to the threat.

H.R. 1731 also directs DHS to scrub the data it receives and add an additional layer of privacy protection. Additionally, it requires the NCCIC to have strong procedures for protecting privacy, and calls for robust oversight by the Department's chief privacy officer, its chief civil rights and civil liberties officer, and inspector general, and the Privacy and Civil Liberties Oversight Board.

I am a cosponsor of H.R. 1731, but as the White House observed earlier this week, improvements are needed to ensure that its liability protections are appropriately targeted. In its current form, it would potentially protect companies that are negligent in how they carry out authorized activities under the act.

Mr. Chairman, before reserving the balance of my time, I wish to engage in a colloquy with the gentleman from Texas (Mr. MCCAUL) regarding the liability protection provisions of H.R. 1731.

At the outset, I would like to express my appreciation for the gentleman's willingness to work with me and the other Democrats on the committee to develop this bipartisan legislation. We have a shared goal of bolstering cybersecurity and improving the quality of information that the private sector receives about timely cyber threats so that they can act to protect their networks and the valuable data stored on them.

Therefore, it is concerning that the liability protection provision appears to undermine this shared goal insofar as it includes language that on its face incentivizes companies to do nothing about actionable cyber information. Specifically, I am speaking of the language on page 36, line 18, that extends liability protections to a company that fails to act on timely threat information provided by DHS or another impacted company.

I would ask the gentleman from Texas to work with me to clarify the language as it moves through the legislative process to underscore that it is not Congress' intent to promote inaction by companies who have timely threat information.

Mr. MCCAUL. Will the gentleman yield?

Mr. THOMPSON of Mississippi. I yield to the gentleman from Texas.

Mr. MCCAUL. Mr. Chair, I thank the gentleman from Mississippi for his question and would say that I do not completely share your view of that clause. I assure you that incentivizing companies to do nothing with timely threat information is certainly not the intent of this provision, as the author of this bill.

On the contrary, I believe it is important that we provide companies with legal safe harbors to encourage sharing of cyber threat information and also believe that every company that participates in this information-sharing process, especially small- and medium-sized businesses, cannot be required to act upon every piece of cyber threat information they receive.

As such, I support looking for ways to clarify that point with you, Mr. THOMPSON. I commit to working with you as this bill moves forward to look for ways to refine the language to ensure that it is consistent with our shared policy goal of getting timely information into the hands of businesses so that they can protect their networks and their data.

□ 0930

Mr. THOMPSON of Mississippi. Mr. Chairman, I reserve the balance of my time.

Mr. MCCAUL. Mr. Chairman, I now yield 5 minutes to the gentleman from Texas (Mr. RATCLIFFE), the chairman of the Subcommittee on Cybersecurity, my close ally and colleague on this legislation.

Mr. RATCLIFFE. I thank the gentleman for yielding.

Mr. Chairman, I am grateful for the opportunity to work with Chairman MCCAUL in crafting the National Cybersecurity Protection Advancement Act. I would also like to thank Ranking Members RICHMOND and THOMPSON for their hard work on this issue; and a special thank you to the Homeland Security staff, who worked incredibly

hard to bring this important bill to the floor today.

Mr. Chairman, for years now, the private sector has been on the front lines in trying to guard against potentially devastating cyber attacks.

Just 2 months ago, one of the Nation's largest health insurance providers, Anthem, suffered a devastating cyber attack that compromised the personal information and health records of more than 80 million Americans.

The consequences of that breach hit home for many of those Americans just a week ago, on tax day, when thousands of them tried to file their tax returns, only to see them be rejected because cyber criminals had used their information to file false tax returns.

Mr. Chairman, attacks like these serve as a wake-up call to all Americans and provide clear evidence that our cyber adversaries have the upper hand. The consequences will get even worse if we fail to tackle this issue head on because even greater and more frightening threats exist, ones that extend to the critical infrastructure that support our very way of life.

I am talking about cyber attacks against the networks which control our bridges, our dams, our power grids, rails, and even our water supply. Attacks on this critical infrastructure have the potential to produce sustained blackouts, halt air traffic, shut off fuel supplies, or, even worse, contaminate the air, food, and water that we need to survive.

These scenarios paint a picture of economic crisis and physical chaos that are, unfortunately, all too real and all too possible right now.

Mr. Chairman, 85 percent of our Nation's critical infrastructure is controlled by the private sector, not by the government, a fact which underscores the reality that America's security, when it comes to defending against cyber attacks, largely depends on the security of our private networks.

The simple truth is that many in the private sector can't defend their networks or our critical infrastructure against these threats.

H.R. 1731 provides a solution for the rapid sharing of important cyber threat information to minimize or, in some cases, prevent the cyber attacks from being successful.

Through the Department of Homeland Security's National Cybersecurity Communication and Integration Center, or NCCIC, this bill will facilitate the sharing of cyber threat indicators between the private sector entities and between the private sector and the Federal Government.

With carefully crafted liability protections, private entities would finally be able to share cyber threat indicators with their private sector counterparts through the NCCIC without fear of liability.

The sharing of these cyber threat indicators, or, more specifically, the tools, techniques, and tactics used by cyber intruders, will arm those who protect our networks with the valuable information they need to fortify our defenses against future cyber attacks.

Because some have said that prior proposals didn't go far enough in safeguarding personal privacy, this bill addresses those concerns with robust privacy measures that ensure the protection of Americans' personal information and private data.

H.R. 1731 will provide protection only for sharing that is done voluntarily with the Department of Homeland Security's NCCIC, which is a civilian entity. It does not provide for or allow sharing with the NSA or the Department of Defense. In fact, this bill expressly prohibits information from being used for surveillance purposes.

This bill also limits the type of information that can be shared, and it requires the removal of all personally identifiable information, which is scrubbed out before the cyber threat indicators can be shared.

In short, this bill improves and increases protection for the personal privacy of Americans, which currently remains so vulnerable to malicious attacks from our cyber adversaries.

Mr. Chairman, the status quo isn't working when it comes to defending against cyber threats. The need to better secure Americans' personal information and better protect and safeguard our critical infrastructure is precisely what compels congressional action right now.

I strongly endorse the passage of this vital legislation, and I urge my colleagues on both sides of the aisle to support it as well. I thank the gentleman from Texas for his leadership.

Mr. THOMPSON of Mississippi. Mr. Chairman, I yield 3 minutes to the gentleman from Rhode Island (Mr. LANGEVIN).

(Mr. LANGEVIN asked and was given permission to revise and extend his remarks.)

Mr. LANGEVIN. I thank the gentleman for yielding.

Mr. Chairman, I am very pleased to be back on the floor today to support the House's second major piece of cybersecurity legislation in less than 24 hours.

As I said yesterday afternoon, it has been a long time coming, for sure. Cybersecurity has been a passion of mine for nearly a decade, and I am absolutely thrilled that, after years of hard work, the House, the Senate, and the President finally are beginning to see eye-to-eye.

The National Cybersecurity Protection Advancement Act has at its core three basic authorizations. First, it authorizes private entities and the DHS's NCCIC to share, for cybersecurity purposes only, cyber threat indicators that have been stripped of personal information and details. Second, it allows businesses to monitor their networks in search of cybersecurity risks. And third, it authorizes companies to deploy limited defensive measures to protect their systems from malicious actors.

Those three authorizations perfectly describe the information-sharing regime we so desperately need. Under the act, companies would collect information on threats, share it with their peers and with a civilian portal, and then use the indicators they have received to defend themselves.

Data are scrubbed of personal identifiable information before they are shared and after they are received by the NCCIC. Companies are offered limited liability protections for sharing information they gather in accordance with this bill.

This legislation also provides for the deployment of rapid automated sharing protocols—something DHS has been hard at work on with the STIX/TAXII program—and it expands last year's NCCIC authorization.

Mr. Chairman, I do believe that the liability protections contained in this bill may prove overly broad, and I certainly hope that we can address that point as the legislative process continues, particularly, hopefully, when we get to a conference committee on this issue.

Overall, though, it is a fine piece of legislation, and I wholeheartedly congratulate Chairman MCCAUL, Ranking Member THOMPSON, Subcommittee Chairman RATCLIFFE, and Ranking Member RICHMOND, as well as the other members of the committee and especially committee staff, for a job well done.

Information-sharing legislation, Mr. Chairman, is not a silver bullet by any means, but it will substantially improve our Nation's cyber defenses and get us to a place where our Nation is much more secure in cyberspace than where we are today.

Protecting critical infrastructure, of course, is among our chief concerns. That will allow for the type of information sharing that will get us to a much more secure place.

So, Mr. Chairman, I urge my colleagues to support this bill, and I hope that the Senate will quickly follow suit.

Mr. MCCAUL. Mr. Chairman, I yield such time as she may consume to the gentlewoman from Michigan (Mrs. MILLER), the vice chairman of the Homeland Security Committee.

Mrs. MILLER of Michigan. Mr. Chairman, first of all, I want to thank the distinguished chairman for yielding the time.

I think you can see by the comments that have been made thus far that we have a very bipartisan bill and a bipartisan approach. That is, through our committee, in no short measure because of the leadership that Chairman MCCAUL and, quite frankly, our ranking member have exhibited with the vision that they have had, these two gentlemen working together, and both the chair and the ranking member on our Subcommittee on Cybersecurity, Mr. RATCLIFFE and Mr. RICHMOND as well.

This really has been a tremendous effort, and so important for our country. This particular issue, obviously, is certainly a bipartisan issue.

I say that, Mr. Chairman, because our Constitution makes the first and foremost responsibility of the Federal Government to provide for the common defense. That is actually in the preamble of our Constitution.

In our modern world, those who are seeking harm to our Nation, to our citizens, to our companies, can use many different means, including attacks over the Internet to attack our Nation.

Recent cyber attacks on U.S. companies like Sony, Target, and Home Depot not only harm these companies, Mr. Chairman, but they harm the American citizens who do business with them, putting their most personal private information at risk.

These threats, as are well known, are coming from nation-states like North Korea, Russia, Iran, China, as well as cyber criminals seeking to steal not only personal information but also intellectual property and sensitive government information.

In today's digital world, we have a duty to defend ourselves against cyber espionage, and the best way to combat these threats is to first recognize the threat and combine private and government resources and intelligence. Mr. Chairman, that is exactly what this bill does.

Mr. Chairman, I think this bill will help to facilitate greater cooperation and efforts to protect our Nation's digital infrastructure, including power grids and other utilities and other services that everyday Americans rely on each and every day.

By removing barriers, which will allow private companies to voluntarily share their cybersecurity threat information with the Department of Homeland Security and/or other companies, I think we will in a very large way improve earlier detection and mitigation of potential threats.

Additionally, this legislation that we are debating on the floor today ensures that personal identification information is removed prior to sharing information related to cyber threats and that very strong safeguards are in place to protect personal privacy and civil liberties.

Mr. Chairman, I point that out because that was something that was discussed a lot by practically every member of the Homeland Security Committee. We were all very, very united on that issue. And I think that is an important critical component, a point to make, and it is reflected in this legislation.

As Mr. RATCLIFFE mentioned just earlier, 85 percent of America's critical infrastructure is owned and operated by the private sector—think about that, 85 percent—which means that cyber threats pose as much of an economic threat to the United States as they do to our security, and we have a constitutional responsibility, as I pointed out in the beginning, to protect ourselves, to protect our Nation, to protect our American citizens from this ever-evolving threat.

So, Mr. Chairman, I would urge that all of my colleagues join me, join all of us on our committee, in voting in favor of this important legislation that will provide an additional line, and a very important line, of defense against cyber attacks.

The CHAIR. The Committee will rise informally.

The Speaker pro tempore (Mr. LOUDERMILK) assumed the chair.

MESSAGE FROM THE SENATE

A message from the Senate by Ms. Curtis, one of its clerks, announced that the Senate has passed a bill of the following title in which the concurrence of the House is requested:

S. 178. An act to provide justice for the victims of trafficking.

The SPEAKER pro tempore. The Committee will resume its sitting.

NATIONAL CYBERSECURITY PROTECTION ADVANCEMENT ACT OF 2015

The Committee resumed its sitting.

Mr. THOMPSON of Mississippi. Mr. Chairman, I yield 2 minutes to the gentleman from Virginia (Mr. CONNOLLY).

Mr. CONNOLLY. I thank my dear friend from Mississippi (Mr. THOMPSON), and I commend him and the distinguished chairman of the committee, Mr. MCCAUL, for their wonderful work on this bill.

Mr. Chairman, we cannot wait. America cannot wait for a cyber Pearl Harbor. This issue—cybersecurity—may be the most complex and difficult challenge we confront long term as a nation.

In the wired 21st century, the line between our physical world and cyberspace continues to blur with every aspect of our lives, from social interaction to commerce. Yet the remarkable gains that have accompanied an increasingly digital and connected society also have opened up new, unprecedented vulnerabilities that threaten to undermine this progress and cause great harm to our country's national security, critical infrastructure, and economy.

□ 0945

It is long overdue for Congress to modernize our cyber laws to address those vulnerabilities present in both public and private networks. The bills before us this week are a step in the right direction, and I am glad to support them, but they are a first step.

Information sharing alone does not inoculate or even defend us from cyber attacks. Indeed, in the critical three P's of enhancing cybersecurity—people, policies, and practices—the measures before us make improvements primarily to policy.

I commend the two committees for working in a bipartisan fashion to improve privacy and transparency protections. More is still needed to safeguard the civil liberties of our constituents.

Further, I hope that the broad liability protections provided by these bills will, in fact, be narrowed upon further consultation with the Senate. Cybersecurity must be a shared public-private responsibility, and that includes the expectation and requirement that our partners will, in fact, take reasonable actions.

Moving forward, I hope Congress will build on this effort to address the security of critical infrastructure, the vast majority of which, as has been already pointed out, is owned and operated by the private sector.

The CHAIR. The time of the gentleman has expired.

Mr. THOMPSON of Mississippi. I yield the gentleman an additional 30 seconds.

Mr. CONNOLLY. We also need to strengthen our Nation's cyber workforce, devise effective data breach notification policies, and bring about a wholesale cultural revolution so that society fully understands the critical importance of good cyber hygiene.

The bottom line is that our vulnerability in cyberspace demands that we take decisive action and take it now, but much like the tactics used in effective cybersecurity, we must recognize that enhancing our cyber defenses is an iterative process that requires continuous effort.

I congratulate the staffs and the leadership of the committee.

Mr. MCCAUL. Mr. Chairman, I yield 5 minutes to the gentleman from Georgia (Mr. LOUDERMILK), a member of the Committee on Homeland Security.

Mr. LOUDERMILK. Mr. Chairman, over the past 40 years, we have experienced advancements in information technology that literally have transformed business, education, government; it has even transformed our culture.

Information research that only a couple of decades ago would take days, months, maybe even years to accomplish is available, quite literally, at our fingertips and instantaneously.

Other aspects of our lives have also been shaped by this immediate access to information. Shopping, you can go shopping without ever going to a store. You can conduct financial transactions without ever going to a bank. You can even have access to entertainment without ever going to a theater.

These advancements in technology have not only transformed the way we access and store information, but it has also transformed the way we communicate.

No longer is instantaneous voice-to-voice communication only available through a phone call, but people around the world instantly connect with one another with a variety of methods, from email, instant text messaging, even video conferencing, and